Eingriffsintensivierung durch Technik

Hannah Ruschemeier 2020-12-16T11:23:16

Am 11.12.2020 veröffentlichte das Bundesverfassungsgericht den Beschluss des Ersten Senats zur erweiterten Datennutzung nach dem Antiterrordateigesetz. Aufgrund der Kombination von Data Mining und der Nutzung einer Verbunddatei von Polizei und Nachrichtendiensten hat das Bundesverfassungsgericht die Vorschrift des § 6a Abs. 2 S. 1 ATDG zu Recht als unverhältnismäßig eingeordnet.

Auch dieser Beschluss – Antiterrordateigesetz II – musste nummeriert werden, denn die Entscheidung setzt die gefühlte Endlosschleife der Sicherheitsgesetzgebung in Deutschland fort: Die Politik entscheidet über immer neue, (teil-)verfassungswidrige Gesetze, welche die Kompetenzen von Polizei und Geheimdiensten ausbauen, damit Karlsruhe die Normen auf das grundrechtskonforme Maß zurechtstutzt (BND, Bestandsdatenauskunft II, Antiterrordatei I; BKAG…).

Antiterrordatei und Data Mining

Die Antiterrordatei dient als Verbunddatei verschiedenen Sicherheitsbehörden zur Bekämpfung des internationalen Terrorismus. Bereits 2013 definierte das Verfassungsgericht klare Vorgaben: Die Antiterrordatei muss im Kern auf eine Informationsanbahnung beschränkt sein und darf eine Nutzung der Daten zur operativen Aufgabenwahrnehmung nur im Ausnahmefall zulassen. Informationsanbahnung ermöglicht zunächst nur den fachrechtlichen Austausch von Erkenntnissen, der andernfalls unpraktikabel oder unmöglich wäre (Antiterrordatei I, Rn. 127).

Nichtsdestotrotz wurde § 6a ATDG, wohl vor allem auf Betreiben der Nachrichtendienste (vgl. Rn. 6), eingeführt. Die Norm erlaubt eine „erweiterte projektbezogene Datennutzung“, sogenanntes Data Mining. Data Mining beschreibt ein computergestütztes statistisches Verfahren, um Muster zu erkennen, Besonderheiten und Zusammenhänge in Daten aufzudecken und gegebenenfalls Prognosen zu erstellen. Es werden dabei entgegen der unpräzisen Bezeichnung keine neuen Daten generiert, sondern Wissen aus vorhandenen Datenbeständen extrahiert. Erhofft wird sich dadurch, dass neue sicherheitsrelevante Erkenntnisse aufgedeckt werden.

Praxisrelevanz hat das Data Mining bisher nicht, da die „notwendigen technischen Rahmenbedingungen“ noch nicht hergestellt sind und dafür auch noch kein Zeitrahmen ersichtlich ist (Rn. 7). Rechtlich relevant ist es dennoch, da sich daraus datenschutzrechtliche Fragen ergeben: Das Bundesverfassungsgericht interveniert hier nicht aufgrund einer „konkreten Gefahr“ für den Datenschutz, sondern bereits aufgrund einer Gefährdungslage. Dadurch festigt es den Maßstab für Grundrechtseingriffe in das Recht auf informationelle Selbstbestimmung (zur Eingriffsrelevanz auch hier).

Eingriffsintensivierung durch technische Ausgestaltung

Das Recht auf informationelle Selbstbestimmung gewährleistet, grundsätzlich selbst über die Preisgabe und Verwendung der eigenen persönlichen Daten zu bestimmen. Darin wird eingegriffen, wenn personenbezogene Informationen von staatlichen Behörden in einer Art und Weise genutzt und verknüpft werden, die für Betroffene nicht ersichtlich oder beeinflussbar sind (Rn. 71, bereits auch Bestandsdatenauskunft II).

Der Eingriff durch die Antiterrordatei liegt zum einen in der weiteren Verwendung vormals getrennter Daten und zudem in dem darüber hinaus gehenden Zugriff, den die erweiterte Nutzung eröffnet (Rn. 73). Das Bundesverfassungsgericht geht davon aus, dass sich durch den Einsatz des Data Minings und den mehrstufigen Analyseschritten die Eingriffsintensität erhöht, da die Verknüpfung das Entstehen neuer Verdachtsmomente erst erzeugt (Rn. 73) – und hält dies für mit der Rasterfahndung vergleichbar. An entsprechend neue Verdachtsmomente können sich wiederum operative Maßnahmen anschließen. Verallgemeinert heißt dies, dass eine zur Datenauswertung eingesetzte „Künstliche Intelligenz“ (KI, z.B. maschinelles Lernen) tendenziell die Eingriffsintensität steigert. Bereits im BND-Urteil führte das Gericht aus, dass gesetzliche Regelungen zum Einsatz von eingriffsintensiven Methoden der Datenauswertung erforderlich seien, insbesondere bei komplexen Formen des Datenabgleichs durch Algorithmeneinsatz (Rn. 192). Die Grundrechtsrelevanz ist aufgrund der möglichen statistischen Analyse großer Datenmengen besonders hoch. Durch KI ergibt sich potenziell eine andere Eingriffsqualität und nicht nur eine Vollzugsoptimierung bisheriger Prozesse, die durch deterministische Systeme vorgenommen werden (zur Eingriffsintensivierung durch Technik im Polizeirecht *Fährmann/Aden*, KrimJ 2/2020, S. 143).

Hinzu kommt im Fall der Antiterrordatei, dass die Grundrechtseingriffe heimlich erfolgen. Die betroffenen Personen haben von ihrer Erfassung in der Datei keine Kenntnis, auch wenn die erweiterte Datennutzung des § 6a ATDG nicht ausschließlich verdeckt gespeicherte Daten umfasst. Bereits erweiterte Grunddaten (vgl. § 3 Abs. 1 Nr. 1 b) ATDG) haben erhebliche Persönlichkeitsrelevanz (Rn. 113). Der Beschluss bestärkt auch die bisherige Rechtsprechung des Bundesverfassungsgerichts zu Abschreckungseffekten auf die Grundrechtsausübung: Selbst, wenn die Nachrichtendienste das Data Mining nur zur informatorischen Aufklärung nutzen, können daraus Erkenntnisse mit erheblicher Persönlichkeitsrelevanz erzeugt werden, die ein „Gefühl des unkontrollierbaren Beobachtetwerdens hervorrufen und nachhaltige Einschüchterungseffekte auf die Freiheitswahrnehmung entfalten“ (Rn. 112, Vorratsdatenspeicherung, Rn. 233; BVerwG 6 C 46.169).

Hypothetische Datenneuerhebung und „informationelles Trennungsprinzip“ als Maßstab der Verhältnismäßigkeit

§ 6a ATDG ermöglicht die erweiterte projektbezogene Datennutzung in abgestufter Form: zur Informationssammlung und -auswertung (Abs. 1), zur Strafverfolgung qualifizierter Straftaten (Abs. 2) und zur Verhinderung solcher (Abs. 3). Die besondere Eingriffsintensität der Befugnisse des § 6a Abs. 2 S. 1 ATDG ergibt sich durch die technische Konzeption des Data Mining und der Nutzung dieser potenziell neuen Erkenntnisse durch Nachrichtendienste und Polizei.

Voraussetzungen für eine zweckändernde Datennutzung

Das Bundesverfassungsgericht verlangte bisher für eine zweckändernde Datennutzung, die sich unmittelbar an eine Datenerhebung anschließt, die Prüfung einer hypothetischen rechtmäßigen Datenneuerhebung. Grundsätzlich gilt, dass jeder Datenumgang, also die Erhebung und Nutzung ein rechtfertigungsbedürftiger Eingriff ist (BVerfGE 150, 244 ff. – KfZ-Kennzeichenkontrollen II. Zum iterativen Grundrechtseingriff: Ruschemeier, Der additive Grundrechtseingriff, 2019, S. 132 ff.). Konzeptionell ist die hypothetische Datenneuerhebung aus dem BKAG bekannt (§ 12 BKAG). Eine weitere Nutzung von Datenbeständen durch staatliche Stellen, die diese nicht selbst erhoben haben, ist nur zulässig, wenn die gesetzliche Grundlage Anlass, Zweck und Umfang sowie entsprechende Eingriffsschwellen präzise normiert (Rn. 98 ff.). Dies gilt auch für den Informationsaustausch verschiedener Behörden untereinander. Durch die Schwelle der hypothetischen Datenneuerhebung soll verhindert werden, dass Daten an Stellen weitergeleitet werden, die ihrerseits strengeren Anforderungen unterliegen als die Behörde, welche die Information übermittelt (bereits Antiterrordateigesetz I, Rn. 114). Eine starre Grenze leitet das Bundesverfassungsgericht daraus nicht ab. Es sollen vielmehr auch Gesichtspunkte der Praktikabilität eine Rolle spielen, so dass die detaillierten Tatbestandsvoraussetzungen für eine Daten*erhebung* nicht ebenfalls spiegelbildlich für die Daten*übermittlung* erforderlich sind. Was „Praktikabilität“ in diesem Kontext genau bedeutet, bleibt unklar. Immerhin müssen bei einer zweckveränderten Datenverarbeitung von Informationen, die durch Wohnraumüberwachung oder den Zugriff auf informationstechnische Systeme generiert wurden, der Konkretisierungsgrad der Gefahrenlage oder der Tatverdacht identisch sein (Rn. 100; BKAG, Rn. 288 ff.).

Daraus ergeben sich Folgefragen für die Grundrechtsprüfung: Sollte in der Zukunft KI für Prognosen aktiviert werden, arbeiten diese Systeme hoch dynamisch, eine Rekonstruktion ihrer Entscheidungsfindung bezieht sich dann auf bereits veraltete Grundannahmen. Es ließen sich weder einzelne Verarbeitungsschritte noch eine Zweckänderung voneinander unterscheiden, da sie unter Umständen nicht rekonstruierbar sind (dazu bereits auch Ralf Poscher). Im konkreten Fall geht das geplante Data Mining erheblich über den ursprünglichen Zweck der Informationsanbahnung der Antiterrordatei hinaus.

Informationsaustausch zwischen Polizei und Nachrichtendiensten: informationelles Trennungsprinzip

Die verfassungsrechtlichen Anforderungen für einen behördlichen Informationsaustausch verschärfen sich bei der Antiterrordatei, da es nicht um eine Informationsübermittlung zwischen zwei Polizeibehörden, sondern um einen Datentransfer zwischen Polizei und Nachrichtendienst geht. Die Sicherheitsarchitektur des Grundgesetzes differenziert klar zwischen der präventiven Polizeitätigkeit, die mit konkreten Eingriffsbefugnissen ausgestattet ist, der Strafverfolgung und dem rein informativ-präventiven Wirken der Nachrichtendienste (vgl. Art. 73 Abs. 1 Nr. 9a, 10, Art. 74 Abs. 1 Nr. 1, Art. 87 Abs. 1 GG; nachrichtendienstliches Trennungsgebot). Unmittelbar bezieht sich die Trennung zunächst nicht auf ihren Informationsaustausch untereinander. Das Bundesverfassungsgericht leitet aus dem Grundrecht auf informationelle Selbstbestimmung aber ein informationelles Trennungsprinzip ab, wonach Daten zwischen den Nachrichtendiensten und Polizeibehörden grundsätzlich nicht ausgetauscht werden dürfen: Der Datenaustausch ist nur unter engen Voraussetzungen ausnahmsweise zulässig (Antiterrordatei I, Rn. 123 ff.).

Nachrichtendienste verfügen über weitreichende Befugnisse zur Datensammlung, die nur an geringe Eingriffsschwellen geknüpft sind, dürfen aber umgekehrt nicht operativ tätig werden. Diese „Vorfeldaufklärung“ findet allerdings auch zunehmend Eingang in die polizeiliche Tätigkeit (exemplarisch dafür ist die gesamte Diskussion um die „drohende Gefahr“, zuletzt hier, insgesamt KrimJ 2/2020). Verfassungsrechtlich problematisch ist die Datenübermittlung bei Nutzung nachrichtendienstlicher Daten durch die Polizeibehörden, die operativ tätig werden können. Im umgekehrten Fall können die durch die Polizei erhobenen Daten deshalb von den Nachrichtendiensten genutzt werden, da diese nicht operativ tätig werden und die Polizeibehörden jedenfalls strengere Anforderungen für die Datenerhebung erfüllen müssen (Rn. 106).

Keine ausreichend konkrete Eingriffsschwelle bei Strafverfolgung

§ 6a Abs. 2 S. 1 ATDG normiert keine hinreichend konkretisierten Eingriffsvoraussetzung für eine erweiterte Datennutzung zur Strafverfolgung, denn es fehlt am gesetzlichen Erfordernis eines konkreten, auf verdichteten Umständen als Tatsachenbasis beruhenden Tatverdachts (Rn. 128). Die Begrenzung auf besonders gewichtige Rechtsgüter sowie Bestimmungen zur Aufsicht und Rechtskontrolle in § 6 Abs. 2 S. 1, Abs. 7 und 8 ATDG können die fehlende Eingriffsschwelle gerade nicht ausgleichen. Dies entspricht der Systematik der StPO, die stets einen Verdacht, wenn auch in unterschiedlichen Abstufungen, als Eingriffsvoraussetzung vorsieht (§ 152 Abs. 2 StPO.). Die „Erforderlichkeit im Einzelfall“ knüpft gerade nicht an die für einen Verdacht notwendige Tatsachengrundlage an und würde deshalb repressive Eingriffsbefugnisse verfassungswidrig erweitern.

Ausreichende Eingriffsschwelle zur Informationsauswertung und zur Verhinderung von Straftaten, § 6a Abs. 1 und 3 ATDG

Die Befugnisse zur erweiterten projektbezogenen Datennutzung in § 6a Abs. 1 und 3 ATD hat das Bundesverfassungsgericht als verfassungskonform angesehen, da im Gegensatz zu Abs. 2 geringere Eingriffsschwellen erforderlich sind.

Nicht operative Tätigkeit als Begrenzung des § 6a Abs. 1 ATDG

Systematisch bezieht sich § 6a Abs. 1 ATDG im Umkehrschluss zu Abs. 2 allein auf eine Informationssammlung und -auswertung (Rn. 125), weshalb auch die Erforderlichkeit im Einzelfall ausreichend ist, denn für Tätigkeiten ohne operative Komponente ist eine niedrigere Eingriffsschwelle erforderlich. Eine explizite Beschränkung auf Nachrichtendienste normiert § 6a Abs. 1 ATDG allerdings nicht. Dadurch sind auch Polizeibehörden umfasst, soweit sie eine Aufgabe wahrnehmen, die allein in der „Sammlung und Auswertung von Informationen“ besteht (darunter fällt z.B. das BKA, soweit es als Zentralstelle für den polizeilichen Informationsverbund befugt ist). Durch die sachliche Begrenzung der Tätigkeit schließt das Gericht somit auch auf einen beschränkten Adressatenkreis. Den Anwendungsbereich des § 6a Abs. 1 ATDG sieht es sachlich auf das Sammeln von Informationen begrenzt, wodurch eine weitergehende Nutzung im Rahmen von Befugnissen zur Gefahrenabwehr und zur Strafverfolgung nachvollziehbar ausgeschlossen ist (Rn. 125).

Verfassungskonforme Auslegung des § 6a Abs. 3 ATDG

Weiterhin ermächtigt § 6a Abs. 3 ATDG die beteiligten Polizeibehörden zur erweiterten Nutzung der Antiterrordatei für die Verhinderung der genannten qualifizierten Straftaten. Als Eingriffsschwelle ist dafür zwar keinen Tatverdacht begründende konkrete Tatsachengrundlage erforderlich, aber eine zumindest hinreichend konkretisierte Gefahr (Rn. 130 und Bestandsdatenauskunft II – Rn. 225 f.). Deshalb kann nach Auffassung des Verfassungsgerichts § 6a Abs. 3 ATDG verfassungskonform dahingehend ausgelegt werden, dass die Erforderlichkeit der Antiterrordateinutzung, um weitere Umstände des Einzelfalls aufzuklären, als konkretisierte Gefahr zu verstehen und nur zulässig ist, „wenn die Behörde bereits ein wenigstens seiner Art nach konkretisiertes und absehbares Geschehen erkennt oder erkennt, dass das individualisierte Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie in absehbarer Zeit terroristische Straftaten begeht“ (Rn. 130 m.w.N.).

Dieser Teil der Entscheidung überzeugt nicht vollständig. § 6a Abs. 3 ATDG ist zwar grundsätzlich enger gefasst sein als die verfassungswidrige erweiterte Nutzung der Antiterrordatei des Abs. 2, da es um die Verhinderung und nicht um die Verfolgung von dort genannten Straftaten geht. Warum die Aufklärung weiterer Zusammenhänge des Einzelfalls in § 6a Abs. 3 ATDG aber verfassungskonform ausgelegt werden kann und dies im Gegensatz zur Strafverfolgung als Eingriffsschwelle hinreichend konkret ist, erschließt sich nicht unmittelbar. Denn auch aus Tätigkeiten mit präventiver Zielrichtung können sich erhebliche Eingriffe ergeben. Das sieht auch das Gericht selbst, wenn es betont, dass diese

konkretisierte Gefahr gerade keine Vor- oder Umfeldermittlungen umfassen darf (Rn. 131 „bei einer solchen Lesart […] verfassungswidrig“).

Abschließende Gedanken und rechtspolitische Einordnung

Das Problem hat sich nicht durch das ATDG erledigt. Die Bestrebungen der Landespolizeibehörden zu groß angelegten Datenanalysen werden aktuell bleiben (z.B. zum Predictive Policing, Übersicht bspw. hier, S. 13 ff.).

Die in der Coronapandemie geäußerte Kritik (z.B. *Lepsius*, RuP 3/2020, S. 273 ff.), dass Grundrechtsschutz nicht erst gegeben ist, wenn Gerichte darüber entscheiden, sondern bei parlamentarischen und exekutiven Entscheidungen stets mitgedacht werden muss, damit der Rechtsstaat funktioniert, ist bereits seit Längerem im Bereich der Sicherheitsgesetze angebracht. Die deutsche Gesetzgebung scheint dem Credo „im Zweifel zu viele Eingriffsbefugnisse“ zu folgen, was mit einem stark durch die Verhältnismäßigkeit akzentuierten Grundrechtsverständnis – „möglichst wenig“, das heißt nur erforderliche Eingriffsbefugnisse“ – widerspricht (zu dieser systemischen Entwicklung der Denormalisierung der Rechtsordnung: Barczak).

Das Bundesverfassungsgericht setzt durch den Beschluss einige wichtige Leitplanken zur Datenerhebung durch die Sicherheitsbehörden. Es wäre wünschenswert, wenn Exekutive und Gesetzgeber bei der nächsten Neuregelung innerhalb dieser Spur bleiben würde. Denn das Verfassungsgericht ist kein Experiemtierlabor für neue Gesetze.

Für hilfreiche Kritik danke ich Thomas Kienle
